I. Obviousness rejection of Claims 1, 3, 5-6, 11, 13, 15, 17, 19, 21-22

Claim 1 recites as follows:

> 1. A security system for a computer connected to a network of computers comprising:
>
> at least one security subsystem associated with said computer, said subsystem being configured to correlate events across a plurality of devices associated with said network of computers and to detect attacks on said computer;
>
> and a secure link between said security subsystem and a master system enabling data communication therebetween; wherein
>
> said master system monitors said security subsystem through said secure link and registers information pertaining to attacks detected by said security subsystem.

The rejection of claim 1 states that Messmer teaches that the black box located on the company network "is configured to correlate events across a plurality of devices associated with the network of computers because Messmer teaches that a probe or "black box sensor" is put on the customer's network to ***accept*** audit data from a wide range of devices" (emphasis added). This statement is squarely contradicted by the Messmer reference itself.

A. Definition of "correlation"

The New Merriam-Webster Dictionary defines the word "correlate" as follows (emphasis added):

> **Correlate:**
>
> Establish the mutual relations of ...

Tech Encyclopedia of the Business Technology Network defines "correlation" (emphasis added) as:

> **Correlation:**
> In statistics, a measure of the strength of the relationship between two variables. It is used to predict the value of one variable given the value of the other. ...

Applicants respectfully remind the Examiner that the correlation function of the present inventive system was extensively discussed during the Examiner's interview on March 12, 2003. Particularly, it was discussed that correlation of events detected on the target network is a part of the overall analysis performed by the entire system, and this particular part is performed by the security subsystem.

B. Network Monitoring Performed by the "Black Box" of Messmer

As disclosed in the cited reference, the "black box" sensor "***captures*** syslog and audit outputs" and "regularly ***transmits*** the network activity output in encrypted form to Counterpane's data centers ..., where it is monitored around the clock." (emphasis added). Therefore, according to the Messmer reference itself, the entire analysis of the ***captured*** and ***transmitted*** data is performed at the operating center, not by the black box. The black box only captures the security-related data and passes it onto the data center.

Additionally, Messmer teaches away from performing any part of the analysis on the target network. It indicates that the analysis of attack footprints can only be performed by trained analysts located in Counterpane's data centers. Moreover, this language suggests that the analysis of attacks is not automated at all but rather fully accomplished by trained analysts.

Therefore, Messmer cannot meet a claim that recites "at least one security subsystem associated with said computer, said subsystem being configured to correlate events across a plurality of devices associated with said network of computers and to

detect attacks on said computer." Thus, Claim 1 is patentably inventive over Messmer. Moreover, none of the other references cited by the Examiner disclose this limitation.

C. Other Rejected Claims

Similarly to Claim 1 above, independent Claims 8, 11, 13, 17, 21 and 22 all include the limitation of performing the correlative part of the analysis at the target network by the security subsystem. Therefore, Claims 8, 11, 13, 17, 21 and 22 are patentably inventive over Messmer. Applicants respectfully submit that dependent Claims 2-7, 9, 10, 12, 14-16, and 18-20 are likewise believed to define patentable subject matter in view of their dependency upon allowable independent Claims and, further, on their own merits.

II. Obviousness rejection of Claims 2, 8, 12, 16 and 20

Claims 2, 8, 12, 16 and 20 have been rejected by the Examiner as unpatentable over Messmer and Newton's Telecom Dictionary, in view of Kurtzberg et al.

Applicants reiterate all arguments presented above with respect to Claim 1 because Claims 2, 8, 12, 16 and 20 all include the limitation of performing the correlative part of the analysis at the target network by the security subsystem, either in their own text or in the text of their base claim. As discussed above, Messmer cannot meet a claim that recites such limitation. Therefore, Claims 2, 8, 12, 16 and 20 are patentably inventive over Messmer.

Moreover, none of the other references cited by the Examiner disclose this limitation.

III. Conclusion

In view of these remarks, Applicant respectfully submits that the claims are in condition for allowance. Applicant requests that the application be passed to issue in due course. The Examiner is urged to telephone Applicant's undersigned counsel at the number noted below if it will advance the prosecution of this application, or with any

suggestion to resolve any condition that would impede allowance. In the event that any extension of time is required, Applicant petitions for that extension of time required to make this response timely. Kindly charge any additional fee, or credit any surplus, to Deposit Account No. 50-0675.

Respectfully submitted,

SCHULTE ROTH & ZABEL

Dated: August 12, 2003

By: Anna Vishev
Anna Vishev
Registration No. 45,018

Mailing Address:
SCHULTE ROTH & ZABEL
919 Third Avenue
New York, New York 10022
(212) 756-2000
(212) 593-5955 Telecopier